

# BANDIT Write-up (L0 -L10)

Bandit is a character in a fictional hacking scenario on a website called [OverTheWire.org](https://OverTheWire.org).

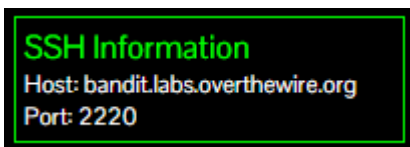
OverTheWire offers a series of wargames designed to teach cybersecurity skills in a safe environment. Bandit is the first wargame in the series, aimed at beginners. It introduces basic *Linux* commands and file manipulation through a series of challenges.

In the Bandit scenario, you play as a new user trying to gain access to higher levels by solving puzzles and cracking passwords. There is no violence or criminal activity involved.

Bandit is the suggested introductory "wargame" within the OverTheWire suite of games. It covers fundamental Linux commands and gradually progresses to advanced techniques as players advance through higher levels. Below are the walkthroughs and methodologies employed to navigate the challenges successfully.

**Note for VMs:** You may fail to connect to overthewire.org via SSH with a "*broken pipe error*" when the network adapter for the VM is configured to use NAT mode. Adding the setting IPQoS throughput to `/etc/ssh/ssh_config` should resolve the issue. If this does not solve your issue, the only option then is to change the adapter to Bridged mode.

## Level 0:



### Bandit Level 0

#### Level Goal

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is **bandit.labs.overthewire.org**, on port 2220. The username is **bandit0** and the password is **bandit0**. Once logged in, go to the [Level 1](#) page to find out how to beat Level 1.

#### Commands you may need to solve this level

ssh

#### Helpful Reading Material

[Secure Shell \(SSH\) on Wikipedia](#)

[How to use SSH on wikiHow](#)

```
(anyway@anyway)~$ ssh bandit0@bandit.labs.overthewire.org -p 2220

Linux am...

      _ _ _ _ _
     | | | | |
     | | | | |
     | | | | |
     | | | | |

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password: 
```

# Level 1:

## Bandit Level 0 → Level 1

### Level Goal

The password for the next level is stored in a file called **readme** located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.

### Commands you may need to solve this level

ls, cd, cat, file, du, find

**TIP:** Create a file for notes and passwords on your local machine!

Passwords for levels are *not* saved automatically. If you do not save them yourself, you will need to start over from bandit0.

Passwords also occassionally change. It is recommended to take notes on how to solve each challenge. As levels get more challenging, detailed notes are useful to return to where you left off, reference for later problems, or help others after you've completed the challenge.

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvYRnrb2rfNWOZOTa6ip5If
```

ZjLjTmM6FvvYRnrb2rfNWOZOTa6ip5If

Log in to each level using the same ssh command, and use the username and flag of the previous level to gain access to the next level.

```
(anyway@anyway)~$ ssh bandit1@bandit.labs.overthewire.org -p 2220
bandit1@bandit.labs.overthewire.org's password: 
```



## Level 2:

### Bandit Level 1 → Level 2

#### Level Goal

The password for the next level is stored in a file called `bandit` - located in the home directory

#### Commands you may need to solve this level

`ls`, `cd`, `cat`, `file`, `du`, `find`

#### Helpful Reading Material

Google Search for "dashed filename"

Advanced Bash-scripting Guide - Chapter 3 - Special Characters

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ ls -la
total 24
-rw-r----- 1 bandit2 bandit1  33 Jul 17 15:57 -
drwxr-xr-x  2 root    root    4096 Jul 17 15:57 .
drwxr-xr-x 70 root    root    4096 Jul 17 15:58 ..
-rw-r--r--  1 root    root     220 Mar 31 08:41 .bash_logout
-rw-r--r--  1 root    root    3771 Mar 31 08:41 .bashrc
-rw-r--r--  1 root    root     807 Mar 31 08:41 .profile
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

263JGJPfgU6LtdEvgfWU1XP5yac29mFx

Listing shows only (-), so use “ls -la” to long list and view hidden files.

- This refers to the current directory.
- This is a wildcard that can match any filename, including hidden files that start with a period (.).

## Level 3:

### Bandit Level 2 → Level 3

#### Level Goal

The password for the next level is stored in a file called **spaces in this filename** located in the home directory

#### Commands you may need to solve this level

ls, cd, cat, file, du, find

#### Helpful Reading Material

Google Search for “spaces in filename”

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat ./spaces\ in\ this\ filename
MnK8KNH3Usiio41PRUEoDFPqfxLPLSmx
bandit2@bandit:~$
```

MNk8KNH3Usii041PRUEoDFPqfxLP1Smx

So, there's a file that contains spaces in its name, we can use (\) this for before spaces to print without error.

## Level 4:

### Bandit Level 3 → Level 4

#### Level Goal

The password for the next level is stored in a hidden file in the **inhere** directory.

#### Commands you may need to solve this level

ls, cd, cat, file, du, find

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x 2 root    root    4096 Jul 17 15:57 .
drwxr-xr-x 3 root    root    4096 Jul 17 15:57 ..
-rw-r----- 1 bandit4 bandit3   33 Jul 17 15:57 ... Hiding-From-You
bandit3@bandit:~/inhere$ cat ..
../
... Hiding-From-You
bandit3@bandit:~/inhere$ cat ... Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
```

2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

# Level 5:

## Bandit Level 4 → Level 5

### Level Goal

The password for the next level is stored in the only human-readable file in the **inhere** directory. Tip: if your terminal is messed up, try the "reset" command.

### Commands you may need to solve this level

ls, cd, cat, file, du, find

```
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls -la
total 48
drwxr-xr-x 2 root    root    4096 Jul 17 15:57 .
drwxr-xr-x 3 root    root    4096 Jul 17 15:57 ..
-rw-r----- 1 bandit5 bandit4  33 Jul 17 15:57 -file00
-rw-r----- 1 bandit5 bandit4  33 Jul 17 15:57 -file01
-rw-r----- 1 bandit5 bandit4  33 Jul 17 15:57 -file02
-rw-r----- 1 bandit5 bandit4  33 Jul 17 15:57 -file03
-rw-r----- 1 bandit5 bandit4  33 Jul 17 15:57 -file04
-rw-r----- 1 bandit5 bandit4  33 Jul 17 15:57 -file05
-rw-r----- 1 bandit5 bandit4  33 Jul 17 15:57 -file06
-rw-r----- 1 bandit5 bandit4  33 Jul 17 15:57 -file07
-rw-r----- 1 bandit5 bandit4  33 Jul 17 15:57 -file08
-rw-r----- 1 bandit5 bandit4  33 Jul 17 15:57 -file09
bandit4@bandit:~/inhere$ file ./-file07
./-file07: ASCII text
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOEOO5pTW81FB8j81xXGUQw
```

So there were 9 files, with each some written text in different formats, we had to find human-readable text in one of the files. We use **file ./-file07** to get the data type in each file. We got ASCII in 7th file, just cat that out:

**4oQYVPkxZOOEOO5pTW81FB8j81xXGUQw**

# Level 6:

## Bandit Level 5 → Level 6

### Level Goal

The password for the next level is stored in a file somewhere under the **inhere** directory and has all of the following properties:

- human-readable
- 1033 bytes in size
- not executable

### Commands you may need to solve this level

ls, cd, cat, file, du, find

```
bandit5@bandit:~$ ls -la
total 24
drwxr-xr-x  3 root root    4096 Jul 17 15:57 .
drwxr-xr-x 70 root root    4096 Jul 17 15:58 ..
-rw-r--r--  1 root root     220 Mar 31 08:41 .bash_logout
-rw-r--r--  1 root root   3771 Mar 31 08:41 .bashrc
drwxr-xr-x 22 root bandit5 4096 Jul 17 15:57 inhere
-rw-r--r--  1 root root     807 Mar 31 08:41 .profile
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls -la
total 88
drwxr-xr-x 22 root bandit5 4096 Jul 17 15:57 .
drwxr-xr-x  3 root root    4096 Jul 17 15:57 ..
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere00
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere01
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere02
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere03
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere04
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere05
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere06
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere07
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere08
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere09
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere10
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere11
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere12
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere13
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere14
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere15
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere16
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere17
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere18
drwxr-xr-x  2 root bandit5 4096 Jul 17 15:57 maybehere19
bandit5@bandit:~/inhere$ find ./ -type f -size 1033c ! -executable 2</dev/null
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HwAsnPhtq9AVKe0dmk45nxy20cvUa6EG
```

**-type f** - filters only regular files.

**-size 1033c** - size must be 1033 (c - bytes).

**! -executable** - filter files only executables.

**2</dev/null** - to hide errors during search.

HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

## Level 7:

### Bandit Level 6 → Level 7

#### Level Goal

The password for the next level is stored **somewhere on the server** and has all of the following properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

#### Commands you may need to solve this level

ls, cd, cat, file, du, find, grep

```
bandit6@bandit:~$ find / -type f -size 33c -user bandit7 -group bandit6 2>/dev/null  
/var/lib/dpkg/info/bandit7.password  
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
```

The command is the same as previous but with some changes:

**Find /** - to find files in sub-directories.

**-user bandit7** - owned by user bandit7

**-group bandit6** - owned by group bandit6

morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj



# Level 8:

## Bandit Level 7 → Level 8

### Level Goal

The password for the next level is stored in the file **data.txt** next to the word **millionth**

### Commands you may need to solve this level

man, grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

```
bandit7@bandit:~$ ls -la
total 4108
drwxr-xr-x  2 root    root      4096 Jul 17 15:57 .
drwxr-xr-x 70 root    root      4096 Jul 17 15:58 ..
-rw-r--r--  1 root    root        220 Mar 31 08:41 .bash_logout
-rw-r--r--  1 root    root      3771 Mar 31 08:41 .bashrc
-rw-r-----  1 bandit8 bandit7 4184396 Jul 17 15:57 data.txt
-rw-r--r--  1 root    root        807 Mar 31 08:41 .profile
bandit7@bandit:~$ cat data.txt | grep "millionth"
millionth      dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
```

So we have **data.txt** and it contains our flags next to a word *millionth*, so we cat that file, and grep that word, it will print out the whole line.

**dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc**

# Level 9:

## Bandit Level 8 → Level 9

### Level Goal

The password for the next level is stored in the file **data.txt** and is the only line of text that occurs only once

### Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

### Helpful Reading Material

Piping and Redirection

```
bandit8@bandit:~$ ls -la
total 56
drwxr-xr-x  2 root    root    4096 Jul 17 15:57 .
drwxr-xr-x 70 root    root    4096 Jul 17 15:58 ..
-rw-r--r--  1 root    root     220 Mar 31 08:41 .bash_logout
-rw-r--r--  1 root    root   3771 Mar 31 08:41 .bashrc
-rw-r-----  1 bandit9 bandit8 33033 Jul 17 15:57 data.txt
-rw-r--r--  1 root    root     807 Mar 31 08:41 .profile
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXDqGana14xvAg0JM
```

So we use **sort** to data.txt, which will sort this text file line by line. And **uniq** finds a unique line in a text file **-u** will remove duplicates.

4CKMh1JI91bUIZZPXDqGana14xvAg0JM

# Level 10:

## Bandit Level 9 → Level 10

### Level Goal

The password for the next level is stored in the file **data.txt** in one of the few human-readable strings, preceded by several '=' characters.

### Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

So, this command will print only printable strings and grep the = sign:

```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ cat data.txt | grep "="
grep: (standard input): binary file matches
bandit9@bandit:~$ cat data.txt | grep =
grep: (standard input): binary file matches
bandit9@bandit:~$ strings data.txt | grep =
-aA"f
\!;===== the
PWAf=1
      M),\}=
2Y6=
G';?e=
===== passwordf
===== isc
*-N6
m=</
E-Bty
-sw
"M1=
===== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
!&-u&4$
*XA=
```

**FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey**

## Flags:

- 1: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5lf
- 2: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx
- 3: MNk8KNH3Usiio41PRUEoDFPqfxLPISmx
- 4: 2WmrDFRmJlq3lPxneAaMGhap0pFhF3NJ
- 5: 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
- 6: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
- 7: morbNTDkSW6jllUc0ymOdMaLnOIFVAaj
- 8: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
- 9: 4CKMh1JI91bUIZZPXqDqGanal4xvAg0JM
- 10: FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey